

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

IN RE APPLICATION OF: Shinobu FUJITA, et al.

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: SEED GENERATING CIRCUIT, RANDOM NUMBER GENERATING CIRCUIT, SEMICONDUCTOR  
INTEGRATED CIRCUIT, IC CARD, AND INFORMATION TERMINAL EQUIPMENT

**REQUEST FOR PRIORITY**

COMMISSIONER FOR PATENTS  
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. Date Filed
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2003-019732	January 29, 2003

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number  
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)
- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.



Marvin J. Spivak

Registration No. 24,913

**C. Irvin McClelland**  
**Registration Number 21,124**

Customer Number

**22850**

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 05/03)



日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 3 年   1 月 2 9 日  
Date of Application:

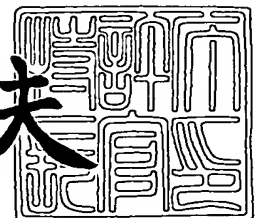
出 願 番 号            特 願 2 0 0 3 - 0 1 9 7 3 2  
Application Number:  
[ST. 10/C]:            [ J P 2 0 0 3 - 0 1 9 7 3 2 ]

出      願      人            株 式 会 社 東 芝  
Applicant(s):

2 0 0 3 年   7 月 1 8 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 PTS0234

【提出日】 平成15年 1月29日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 7/58

【発明の名称】 シード生成回路、乱数生成回路、半導体集積回路、I C  
カード及び情報端末機器

【請求項の数】 13

【発明者】

【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝  
研究開発センター内

【氏名】 藤田 忍

【発明者】

【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝  
マイクロエレクトロニクスセンター内

【氏名】 岩村 鉄郎

【特許出願人】

【識別番号】 000003078

【氏名又は名称】 株式会社 東芝

【代理人】

【識別番号】 100088487

【弁理士】

【氏名又は名称】 松山 允之

【選任した代理人】

【識別番号】 100108062

【弁理士】

【氏名又は名称】 日向寺 雅彦

【手数料の表示】

【予納台帳番号】 087469

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 シード生成回路、乱数生成回路、半導体集積回路、ICカード及び情報端末機器

【特許請求の範囲】

【請求項 1】

連続的または断続的に発振する発振回路と、  
前記発振回路から出力されたデジタルデータ列における「0」と「1」との出現頻度を制御して時系列データとして出力する平滑回路と、  
前記時系列データのうちの複数のビットを用いた演算処理により、1ビットのシードを生成する真性化回路と、  
を備えたことを特徴とするシード生成回路。

【請求項 2】

前記発振回路は、入力された複数のデータが特定の組み合わせとなった場合のみ発振することを特徴とする請求項 1 記載のシード生成回路。

【請求項 3】

前記発振回路は、2つの排他的論理和演算回路と2つの反転回路をそれぞれ交互に直列接続し、前記2つの排他的論理和演算回路のそれぞれの入力的一端に、前記複数のデータのそれぞれを与えるものであることを特徴とする請求項 2 記載のシード生成回路。

【請求項 4】

前記発振回路は、リング発振回路を含み連続的に発振することを特徴とする請求項 1 記載のシード生成回路。

【請求項 5】

前記平滑回路は、  
擬似乱数を生成する擬似乱数生成手段と、  
前記発振回路から出力された前記デジタルデータ列と、前記擬似乱数生成手段により生成された前記擬似乱数と、の排他的論理和を演算して前記時系列データとして出力する論理演算手段と、  
を有することを特徴とする請求項 1～4 のいずれか 1 つに記載のシード生成回

路。

**【請求項 6】**

前記平滑回路は、その出力において、前記発振回路から出力されたデジタルデータ列よりも「0」と「1」との出現頻度が1:1に近いことを特徴とする請求項1～5のいずれか1つに記載のシード生成回路。

**【請求項 7】**

前記真性化回路は、前記演算処理を行う排他的論理和演算回路を有することを特徴とする請求項1～6のいずれか1つに記載のシード生成回路。

**【請求項 8】**

前記真性化回路は、前記複数のビットの組み合わせに応じて「0」及び「1」のいずれかを割り当てるテーブルに基づいて前記1ビットのシードを生成することを特徴とする請求項1～6のいずれか1つに記載のシード生成回路。

**【請求項 9】**

請求項1～8のいずれか1つに記載のシード生成回路と、  
前記シード生成回路により生成された前記シードに基づいて擬似乱数を生成する擬似乱数生成回路と、  
を備えたことを特徴とする乱数生成回路。

**【請求項 10】**

デジタル入力値に対して一義的に決定されないデジタル出力値を与える不確定論理回路をさらに備え、  
前記擬似乱数を前記不確定論理回路に入力して、その出力を乱数として出力することを特徴とする請求項9記載の乱数生成回路。

**【請求項 11】**

請求項9または10に記載の乱数生成回路を備えたことを特徴とする半導体集積回路。

**【請求項 12】**

請求項11記載の半導体集積回路を備えたことを特徴とするICカード。

**【請求項 13】**

請求項11記載の半導体集積回路を備えたことを特徴とする情報端末機器。

**【発明の詳細な説明】****【0001】****【発明の属する技術分野】**

本発明は、シード生成回路、乱数生成回路、半導体集積回路、ICカード及び情報端末機器に関し、特に、デジタル論理回路によりコンパクトに構成することが可能でしかも真性度が高い乱数のシードを生成し、暗号アルゴリズムに用いても好適なシード生成回路及びこれを用いた乱数生成回路、半導体集積回路、ICカード及び情報端末機器に関する。

**【0002】****【従来の技術】**

確率過程を伴う現象のシミュレーションや各種のセキュリティーのために乱数列を用いる場合、時系列にみた乱数性だけではなく、時系列に並べられた乱数列から同一クロックで取得したデータにおける乱数性も重要である。なぜなら同一クロックで多数データサンプリングすることで、暗号情報を読み取る手口が存在し、その暗号データを乱数と演算処理することで、読み取られにくくする方法に乱数が使われるからである。

**【0003】**

擬似乱数生成回路は比較的小型であり、それにより得られた時系列のデータは、比較的高品質な乱数として用いることが可能である。しかし、電源を投入してシステムをオン（ON）した後に同一クロックで取得したデータを1回目、2回目・・・と順番に並べたデータ自体においては、十分な乱数性が保証できない。

**【0004】**

図16は、この事情を説明するための概念図である。すなわち、擬似乱数生成回路を含むシステムをオンにする度に、「0」と「1」とが時系列に出力されて乱数列が生成されるものとする。この時、それぞれの乱数列を時系列（すなわち、同図の横軸方向）にみた場合の乱数性は良好である。しかし、これら乱数列から同一クロックで特定のデータをサンプリングした（同図の縦軸方向にみた）場合、そのデータ系列の乱数性は必ずしも良質とはいえない。例えば、図16に例示したように、同一クロックデータ列においては、「0」または「1」のいずれ

かの出現頻度が高いというような問題が生ずる。これは、擬似乱数の場合には、擬似乱数回路の「初期値」すなわち「シード」に依存して乱数列が決定されるからである。

#### 【0 0 0 5】

図 1 7 は、擬似乱数回路におけるシードの役割を説明するための概念図である。すなわち、同図（a）は、擬似乱数回路の一例であるリニア・フィードバック・シフトレジスタを用いた回路を表す。この回路においては、入力されたシードに応じて、データ X が順次出力される。しかし、入力されるシードが固定されていれば、得られる乱数列（同図の横方向の列）も同一である。従って、これら乱数列から同一クロックでサンプリングされて得られる同一クロックデータ列（同図の縦方向の列）は、常に同じデータの配列となってしまう。

#### 【0 0 0 6】

仮に、これを「乱す」役割を有する何らかの回路を設けたとしても、同一クロックデータ列は良質の乱数にはなりにくい。すなわち、入力されるシードを毎回、書き換えたとしても、同図（c）に表したように、「0」と「1」とのバランスが 1：1 からずれたり、何らかの規則性や周期性が存在したりする場合が多い。これは、擬似乱数回路の同一クロックデータ列のランダム性は、入力されるシードのランダム性だけに依存するからである。つまり、擬似乱数回路の場合、入力されるシードのランダム性が極めて重要となる。

#### 【0 0 0 7】

起動時に書き換えられるシードが、ソフト的に書き換える場合も多いが、これでシード自身に常に違った乱数性を与えるのはほとんど不可能である。例えば、特許文献 1 には、「移動体端末の有する機能手段が発生する状態情報のうちで時間的に不規則に変化する再現性のない情報の一部を抽出してサンプルデータとする。サンプルデータをシード 1 0 2 として乱数生成部 1 0 3 に入力して、乱数 1 0 4 を発生する。」方法が開示されている。

#### 【0 0 0 8】

#### 【特許文献 1】

特開 2 0 0 2 - 2 1 5 0 3 0 号公報



**【発明が解決しようとする課題】**

しかし、特許文献1に開示された技術による場合、サンプルデータ自体にはランダム性はあっても、「0」と「1」のバランスを保つような仕組みや、周期性規則性が存在しないような仕組みが設けられていない。

**【0009】**

これに対して、擬似乱数回路においては、シードを常にランダムに書き換える機構が必要である。つまり、ハード的に出現する何らかのランダムネスを利用し、しかも「0」と「1」とのバランスが1:1からずれておらず、規則性や周期性を持たないランダムなシードを作り出す必要がある。

**【0010】**

熱雑音等の純粋物理現象で発生するランダム信号を利用して、乱数を作り、これをシードに利用する手段もあるが、一般的に大型の回路となってしまうため、例えば、半導体集積回路やICカードあるいは各種の情報端末機器などの小型のシステムに内蔵することが困難である。

**【0011】**

本発明は、かかる課題の認識に基づいてなされたものであり、その目的は、乱数性の高いシードを生成し、かつ小型の集積回路化が可能なシード生成回路及びこれを用いた乱数生成回路、半導体集積回路、ICカード及び情報端末機器を提供することにある。

**【課題を解決するための手段】**

上記目的を達成するため、本発明のシード生成回路は、連続的または断続的に発振する発振回路と、前記発振回路から出力されたデジタルデータ列における「0」と「1」との出現頻度を制御して時系列データとして出力する平滑回路と、前記時系列データのうちの複数のビットを用いた演算処理により、1ビットのシードを生成する真性化回路と、を備えたことを特徴とする。

**【0012】**

上記構成によれば、乱数性の高いシードを生成し、かつ小型の集積回路化が可能なシード生成回路を実現できる。

**【0013】**

ここで、前記発振回路は、入力された複数のデータが特定の組み合わせとなった場合のみ発振するものとすることができる。

#### 【0014】

またこの場合、前記発振回路は、2つの排他的論理和演算回路と2つの反転回路をそれぞれ交互に直列接続し、前記2つの排他的論理和演算回路のそれぞれの入力的一端に、前記複数のデータのそれぞれを与えるものとしてもよい。

#### 【0015】

また、前記発振回路は、リング発振回路を含み連続的に発振するものとすることもできる。

#### 【0016】

一方、前記平滑回路は、擬似乱数を生成する擬似乱数生成手段と、前記発振回路から出力された前記デジタルデータ列と、前記擬似乱数生成手段により生成された前記擬似乱数と、の排他的論理和を演算して前記時系列データとして出力する論理演算手段と、を有するものとすることができる。

#### 【0017】

また、前記平滑回路は、その出力において、前記発振回路から出力されたデジタルデータ列よりも「0」と「1」との出現頻度が1:1に近いものとすることが望ましい。

#### 【0018】

一方、前記真性化回路は、前記演算処理を行う排他的論理和演算回路を有するものとすることができる。

#### 【0019】

また、前記真性化回路は、前記複数のビットの組み合わせに応じて「0」及び「1」のいずれかを割り当てるテーブルに基づいて前記1ビットのシードを生成するものとすることもできる。

#### 【0020】

一方、本発明の乱数生成回路は、上記いずれかのシード生成回路と、前記シード生成回路により生成された前記シードに基づいて擬似乱数を生成する擬似乱数生成回路と、を備えたことを特徴とする。

**【0021】**

上記構成によれば、乱数性の高いシードを生成し、かつ小型の集積回路化が可能な乱数生成回路を実現できる。

**【0022】**

ここで、デジタル入力値に対して一義的に決定されないデジタル出力値を与える不確定論理回路をさらに備え、前記擬似乱数を前記不確定論理回路に入力して、その出力を乱数として出力するものとすることができる。

**【0023】**

一方、本発明の半導体集積回路は、上記いずれかの乱数生成回路を備えたことを特徴とする。上記構成によれば、乱数性の高いシードを生成し、かつ小型の集積回路化が可能な半導体集積回路を実現できる。

**【0024】**

一方、本発明のＩＣＩＣカードは、上記の半導体集積回路を備えたことを特徴とする。上記構成によれば、コンパクトで高いレベルのセキュリティが得られしかも低コストのＩＣカードを実現できる。

**【0025】**

一方、本発明の情報端末機器は、上記の半導体集積回路を備えたことを特徴とする。上記構成によれば、上記構成によれば、コンパクトで高いレベルのセキュリティ及び暗号処理技術が得られしかも低コストのＩＣカードを実現できる。

**【0026】****【発明の実施の形態】**

以下、図面を参照しつつ、本発明の実施の形態について詳細に説明する。

**【0027】**

図１は、本発明の実施の形態にかかるシード生成回路の要部構成を表すブロック図である。すなわち、本実施形態のシード生成回路は、発振回路１０と、平滑回路２０と、を有する。

**【0028】**

発振回路１０は、連続的または断続的（非連続的）に発振することによってランダム信号を発生する回路である。ランダム信号を作るのに発振を利用するのは

、小型化が容易だからである。一方、平滑回路 20 は、発振回路 10 から出力されたランダム信号の「0」と「1」とのバランスをとり、かつその周期性や規則性を壊す回路である。このような構成により、「0」と「1」とのバランスを時系列的に一様にすることができる。さらに、時系列的に生成した多数ビットを使って、所定の演算処理により、1 ビットのランダムな擬似乱数用のシードを生成することができる。

#### 【0029】

図 2 は、発振回路 10 の具体例を表す模式図である。すなわち、本具体例の発振回路は、2 つの入力 X 1、X 2 に対して、2 つの出力 Q 1、Q 2 を与える。2 つの入力 X 1、X 2 の値が同じ場合には、偶数インバータを備えたフリップフロップと等価の動作をする。一方、2 つの入力 X 1、X 2 が異なる場合には、リング発振する回路である。従って、2 つの入力 X 1、X 2 の値が同じ場合と異なる場合との割合が半々であれば、回路動作期間の半分の期間だけ発振する。

#### 【0030】

またさらに、図 2 の回路は、単純な発振回路とは異なり、初期値 Z の値によっても出力が異なる。すなわち、初期値 Z が「1」の場合には、入力 X 1、X 2 がいずれも「1」の時には出力 Q 1、Q 2 はいずれも「0」となり、入力 X 1、X 2 がいずれも「0」の時には出力 Q 1 は「1」、Q 2 は「0」となる。

#### 【0031】

一方、初期値 Z が「0」の場合には、入力 X 1、X 2 がいずれも「1」の時には出力 Q 1、Q 2 はいずれも「1」となり、入力 X 1、X 2 がいずれも「0」の時には出力 Q 1 は「0」、Q 2 は「1」となる。

#### 【0032】

このように、図 2 の具体例の発振回路 10 は、2 つの入力 X 1、X 2 が異なる場合にのみ発振する点で、「断続的発振回路」であるといえる。連続的発振回路は、乱数データに周期性が残りやすいという点と、消費電流が大きいという点が弱点であり、断続的発振回路は、この点を改善した回路である。

#### 【0033】

一方、図 3 は、発振回路 10 のもう一つの具体例を表す模式図である。すなわ

ち、本具体例の発振回路は、3つのインバータを直列接続したリング発振器であり、「連続的発振回路」であるといえる。この場合、発振周波数は、概ねシステムクロックの10倍以上であることが望ましい。

#### 【0034】

次に、本発明における平滑回路20について説明する。

#### 【0035】

図4は、本発明における平滑回路20の基本的な構成を表すブロック図である。すなわち、平滑回路20は、擬似乱数出力手段20Aと、XOR（排他的論理和）演算手段20Bとを有する。擬似乱数出力手段20Aとしては、例えば、リニア・フィードバック・シフト・レジスタ（Linear Feedback Shift Resistor：LFSR）などを用いることができる。

#### 【0036】

このようにして、発振回路10から得られたランダム信号と、擬似乱数出力とのXOR（排他的論理和）を取ることにより、ランダム信号の一様性を著しく改善することができる。ただしこの場合、発振回路10と擬似乱数出力20Aとの出力の間に相関性がないことが望ましい。以下、この点について詳述する。

#### 【0037】

まず、独立した2つの回路からの出力をQ1、Q2とする。Q1、Q2には相関が無いとする。このとき、Q1における「1」の出現比率をp、Q2における「1」の出現比率をqとする。すると、Q1とQ2とをXORした出力Rが「1」となる出現比率rは、以下の式で与えられる。

#### 【0038】

$$r = p + q - 2pq \quad (1)$$

XOR出力における「1」と「0」との出現比率の差は、次式により与えられる。

#### 【0039】

$$|r - (1 - r)| = |(1 - 2p)(1 - 2q)| \quad (2)$$

Q1とQ2の出力における「1」と「0」の出現比率の差は、それぞれ、 $|1 - 2p|$ 、 $|1 - 2q|$ であり、 $p$ と $q$ はともに、0以上1以下なので、次式が得られる。

【0040】

$$|(1 - 2p)(1 - 2q)| < |1 - 2p|, |1 - 2q| \quad (3)$$

これは、XORする前よりも、XORした後のほうが、「0」と「1」の出現比率の差が小さくなること、つまり「偏り」が小さくなることを表している。従って、複数個のデータを並列化してXORしていくと、単独の出力よりも「偏り」が小さくなる。例えば、出力が偏った回路が多数あっても、出力の「偏り」の小さいものが一つでも存在すれば、その一つの回路出力よりもさらに「偏り」が小さい出力が得られることになる。

【0041】

一方、相関がある場合には、次のようになる。すなわち、独立した2つの回路からの出力をQ1、Q2とする。Q1、Q2には何らかの理由で相関があるとする。このとき、Q1の1の出現比率を $p$ 、Q2のそれを $q$ とする。Q1とQ2に相関がある場合には、Q1が「1」の場合に、Q2が「1」となる確率は、単純に $q$ ではなく、 $\phi$ の割合だけずれるとする。 $\phi$ が「1」からずれている度合いが相関性を表す。

【0042】

そうすると、出現確率は以下の如くとなる。

【0043】

Q1が「1」の場合に、Q2が「1」となる確率 $= p q \phi$

Q1が「1」の場合に、Q2が「0」となる確率 $= (1 - q) \phi p$

Q1が「0」の場合に、Q2が「1」となる確率 $= q (1 - \phi p)$

Q1が「0」の場合に、Q2が「0」となる確率 $= (1 - q) (1 - \phi p)$

## 【0044】

Q1とQ2とをXORした出力Rについて、「1」（Q1とQ2が等しくない）の出現比率rは、次式により与えられる。

## 【0045】

$$r = (1 - q) \phi p + q (1 - \phi) \quad (4)$$

出力Rにおける「1」と「0」の出現比率の差は、次式により得られる。

## 【0046】

$$|r - (1 - r)| = |1 - 2\phi p| |1 - 2q| \quad (5)$$

つまり、相関がある場合、Q1とQ2のXOR=Rでは、Q1、Q2の1の出現確率は、pとqだけでなく、相関の度合い $\phi$ にも影響を受ける。そして、pとqがそれぞれ「0.5」に近い値の場合は、次式により表される。

## 【0047】

$$|r - (1 - r)| = |1 - \phi| \quad (6)$$

ここで相関性が無い場合は $\phi$ が「1」となり、「0」と「1」は均一となる。逆に、相関が強く $\phi$ が「0」または「2」程度になると、Rはほとんど全て「1」または「0」となってしまう。

## 【0048】

従って、平滑回路20においてXORを演算する場合には、その2つの入力Q1とQ2に相関性を持たせないようにする工夫が必要である。つまり、発振回路10と擬似乱数出力手段20Aとの間に相関性が生じないようにすることが望ましい。

## 【0049】

例えば、これら2つの回路に、同じクロックをダイレクトに入力しないことが

望ましい。アナログ的な動作をする回路の場合には、Q1とQ2の出力端も別個にラッチすることが望ましい。発振回路10と擬似乱数出力手段20Aは、これらの点に気をつけて設計する必要がある。

#### 【0050】

以上、平滑回路20が有する、一様化の作用について詳述した。

#### 【0051】

一方、平滑回路20は、同一クロックデータ列における周期性を乱す作用も有する。すなわち、出力を時系列に並べると、FIPS140-2検定を通る乱数があるとする。しかし、このような乱数をもとにして、ある時間で発生した1ビットを単純にシードにするだけでは、同一クロックでのランダムネスが十分に得られない。そこで、本発明においては、時系列的に生成した多数ビットを使って1ビットの乱数データを作る。その典型的なものは、複数データの全てにXORを取ることである。つまり、時系列データをX1, X2, X3...Xnとした場合、次式により、n個の時系列データから1ビットの乱数データを作る。

#### 【0052】

##### 【数1】

$$W_1 = X_1 \oplus X_2 \oplus X_3 \oplus \dots \oplus X_n \quad (7)$$

これは、一様性に関して前述したものと同様の効果によって、「0」と「1」との出現確率の均一性（一様性）を向上する方法である。これは時系列での効果であるが、複数の時系列データから同一クロックでサンプリングして得られた同一クロックデータ列における乱数性を上げる効果もあることが分かる。この点について、以下に説明する。

#### 【0053】

すなわち、前述したように、シードが固定である場合、LFSRの出力データにおいては、同一クロックでは常に同じデータが並ぶ。時系列データがX1, X2, X3...Xnの場合、同一クロックのデータに関する予測確率をそれぞれf1, f2, f3...fnとする。ここで予測確率は、「0」と「1」の出現



確率をそれぞれ  $(0.5 + f_k)$ ,  $(0.5 - f_k)$  と定義することにする。LFSR の場合、全て予測可能なので、次式が与えられる。

【0054】

$$f_k = \pm 0.5 \quad (k = 1, 2 \dots n) \quad (8)$$

同一クロック配列が乱数性を持つことは、 $f_k$  が「0」に近づくこと、つまり予測困難であることを意味する。

【0055】

いま、クロックの異なる二つの出力  $X_j$ ,  $X_h$  を選び、この XOR を  $X_{jh}$  とする。

【0056】

【数2】

$$X_{jh} = X_j \oplus X_h$$

例えば、 $X_j$  の予測確率が「0.4」、 $X_h$  の予測確率が「0.3」である場合を考える。 $X_{jh}$  が「1」となるのは、 $X_j = 1$ 、 $X_h = 1$  または  $X_j = 0$ 、 $X_h = 1$  の場合である。従って、その確率は、 $0.9 \times (1 - 0.8) + (1 - 0.9) \times 0.8 = 0.26$  であり、予測確率  $f_{jh}$  は「0.24」である。つまり、 $X_j$  と  $X_h$  の排他的論理和 (XOR) の予測確率  $f_{jh}$  は、 $X_j$ 、 $X_h$  の予測確率  $f_j$ ,  $f_h$  よりも小さい。つまり、排他的論理和をとることによって、予測困難性が上がっていることが分かる。これを一般的に表すと、 $X_j$  と  $X_h$  排他的論理和  $X_{jh}$  の予測確率  $f_{jh}$  は、次式の如くとなる。

【0057】

$$\begin{aligned} f_{jh} &= 0.5 - (0.5 + f_j)(0.5 - f_h) - (0.5 - f_j)(0.5 + f_h) \\ &= 2 f_j \times f_h \end{aligned} \quad (9)$$

$f_j$ ,  $f_h$ は、共に絶対値が「0.5」よりも小さいので、 $X_j$ と $X_h$ の排他的論理和 $X_{jh}$ の予測確率 $f_{jh}$ は $X_j$ ,  $X_h$ の予測確率 $f_j$ ,  $f_h$ よりも小さいことが一般的に証明できる。従って、排他的論理和をとる時系列のデータ数を重ねていくほど、同一クロックにおけるデータ列の予測確率が小さくなっていく。その結果として、複数の時系列データから同一クロックでサンプリングした同一クロックデータ列における周期性を低下させ、良質のシードを与えることができる。

#### 【0058】

以上、平滑回路20について説明した。

次に、真性化回路30について説明する。

#### 【0059】

図5は、真性化回路30の作用を説明するための模式図である。すなわち、真性化回路30は、平滑回路20から出力された乱数列を演算処理し、1ビットのシードを生成する。その具体的な構成については、以下に具体例を参照しつつ説明する。

#### 【0060】

(第1の具体例)

図6は、本発明の第1の具体例にかかるシード生成回路を表すブロック図である。すなわち、このシード生成回路は、図2に表した発振回路10を備えている。前述したように、この発振回路10は、「断続的発振回路」であり、2つの入力 $X_1$ 、 $X_2$ が異なる場合のみ、リング発振する。そして、これら2つの入力 $X_1$ 、 $X_2$ の値が同じ場合と異なる場合が半々であれば、回路動作時の半分の時間だけ発振する。

#### 【0061】

一方、平滑回路20は、擬似乱数出力手段20Aとして、13段のシフトレジスタを有するLFSRを設けることができる。そして、発振回路10とLFSRの出力とを平滑回路20においてXORを演算することにより、例示したような乱数列が得られる。

#### 【0062】

一方、真性化回路 3 0 は、このように時系列的に生成される多数ビットの X O R を演算することにより、1 ビットのシードを生成する。この回路を n クロック分だけ動作させると、n ビットの時系列データの X O R が Q に出力される。

#### 【 0 0 6 3 】

本具体例のシード生成回路の場合、必要な論理ゲート数は、周辺回路を含めても約 5 0 ゲート程度であり、回路規模は小さい。入力 X 1 として、ロー ( L o w ) レベルかハイ ( H i g h ) レベルに固定した値を入力し、X 2 としては基準クロックを入力する。これにより、発振 ( 不確定出力 ) と確定出力とを交互に繰り返す動作が実行される。この場合、クロックは、他の回路用のクロックと同期していても良く、または非同期でも良い。

#### 【 0 0 6 4 】

本具体例のシード生成回路を作製して 6 4 クロック分の時系列データの X O R 出力を 2 0 0 0 0 個 ( 同一クロックデータ列 ) 取得して、これを統計的な検定にかけた。図 7 は、この結果を表す一覧表である。すなわち、同図には、技術標準局 ( N I S T ) による検定規格 F I P S 1 4 0 - 2 と、棄却率 5 % の一般検定の結果を表した。また、図 7 には、比較例として、熱雑音増幅型の物理乱数回路を用いた場合の結果と、1 6 段の L F S R から得られた結果も表した。

#### 【 0 0 6 5 】

図 7 から分かるように、本具体例のシード生成回路によれば、同一クロックの 1 ビットのシード列 ( 同一クロックデータ列 ) においても、F I P S 1 4 0 - 2 の検定だけでなく、棄却率 5 % の難解な一般検定もクリアする良好な乱数性が得られることが確認された。物理乱数回路の場合、時系列データと同一クロックデータ列とは基本的に同一である。一方、L F S R の場合は、シードが固定されているので同一クロックデータ列においてはいつも同じデータが並ぶため、当然ながら全ての検定は不合格となる。

#### 【 0 0 6 6 】

図 8 は、8 個のシード生成回路について、システム起動後のクロック数と乱数データの各 1 ビットについて、一様性の改善の傾向を表すグラフ図である。同図から、クロック数が増すほど一様性が改善されることが確認された。なお、発振

回路 10 は消費電流が比較的大きいので、ある程度のランダム性をもつ出力データが得られたら、そのデータを平滑回路 20 に受け渡し、発振回路 10 は停止させればよい。

#### 【0067】

(第2の具体例)

図9は、本発明の第2の具体例にかかるシード生成回路を表す模式図である。本具体例においては、発振回路 10 として、図3に表したリング発振器を用いている。つまり、本具体例は、「連続的発振回路」を用いたシード生成回路であるといえる。この場合、発振回路の発振周波数は、概ねシステムクロックの10倍以上が望ましい。前述したように、発振回路 10 のリング発振回路は、他の回路と非同期とすることが望ましい。

#### 【0068】

一方、平滑回路 20 は、擬似乱数生成回路 20A と、XOR 演算手段 20B と、を有する。擬似乱数生成回路 20A は、11 段のシフトレジスタからなる LFSR の最下位 2 ビットの論理積 (AND) と、次位の 1 ビットの反転との論理和 (OR) をとって、最上位の 1 ビットと XOR したものを最下位のシフトレジスタに戻す回路であり、非線形の擬似乱数生成回路であるといえる。

#### 【0069】

リング発振器の出力と、擬似乱数生成回路 20A の出力と、を XOR 演算手段 20B において演算し、時系列に発生するランダムデータ列を得る。

#### 【0070】

このランダムデータ列は、真性化回路 30 において処理され、1 ビットのシードが得られる。真性化回路 30 においては、図示したように、データ列のうちで続いた 2 ビットが「01」または「10」というように、違った数字が並ぶ場合には、「1」に変換し、一方、続いた 2 ビットが「11」または「00」というふうに、同じ数字が並ぶ場合には、「0」に変換する処理を実行する。これを 1 ビットになるまで繰り返し、1 ビットのシードを生成する。

#### 【0071】

(第3の具体例)

次に、本発明の第3の具体例として、真性化回路30における処理の変型例を説明する。

#### 【0072】

図10は、本具体例にかかるシード生成回路を表す模式図である。本具体例の場合、平滑回路20において、4の倍数すなわち $4^n$ 個の時系列データを生成させておく（ $n$ は任意の数）。この時系列データを真性化回路30において4個のデータの組み合わせ毎にそれぞれ図示したように分類して、「0」または「1」に変換する。これを $n$ 回繰り返して1ビットを作る。

#### 【0073】

このように、 $n$ ビットを1ビットに変換するテーブル（変換表）を用意しておき、このテーブルに対応する変換を実行するための変換回路を論理回路で作製すれば真性化回路30が得られる。このとき、テーブルは、「0」と「1」とが等しい確率で変換されるように作られなければならない。それが満たされていれば、どんなテーブルでも良い。

#### 【0074】

（第4の具体例）

次に、本発明の第4の具体例として、本発明のシード生成回路を備えた乱数生成回路について説明する。

#### 【0075】

図11は、本具体例にかかる乱数生成回路を表す模式図である。すなわち、この乱数生成回路100は、シード生成回路110と、擬似乱数生成回路120と、不確定論理回路130と、を有する。

#### 【0076】

シード生成回路110は、図1乃至図10に関して前述したような本発明のシード生成回路である。擬似乱数生成回路120は、例えば、LFSRなどを用いて擬似乱数を生成する回路である。

#### 【0077】

一方、不確定論理回路130としては、本発明者が特願2002-183967号において開示した不確定論理回路を用いることができる。この回路は、デジ

タル入力値に対して一義的に決定されないデジタル出力値を与える。すなわち、特定の入力信号の組み合わせに対して出力の「0」または「1」が不確定になる作用を有する。論理出力が不確定の場合、不確定論理回路 10 を構成する素子のその時々物理的な要因によって、出力が変動する。この物理現象を利用することにより、一定の入力に対して、出力が変動する（不確定となる）デジタル回路が得られ、「0」と「1」とのランダムなデジタル信号列が得られる。

#### 【0078】

本具体例の乱数生成回路 100 の場合、シード生成回路 110 により生成されたシードが擬似乱数生成回路 120 に入力されて擬似乱数が生成される。そして、擬似乱数生成回路 120 が持っている周期性を不確定論理回路 130 により壊す。この結果、得られる乱数の質がより高品質になる。不確定論理回路 130 を合体すると回路規模自体は凡そ 2 倍になるが、それでもせいぜい 1000 ゲート程度であるので、後に詳述するように、IC（半導体集積回路）、IC カード用チップ、小型携帯端末などに搭載可能である。

#### 【0079】

（第 5 の具体例）

次に、本発明の第 5 の具体例として、本発明のシード生成回路を設けた半導体集積回路（IC）について説明する。

#### 【0080】

図 12 は、本具体例の半導体集積回路の要部構成を表す模式図である。本具体例は、例えば IC カードなどに搭載することができる IC であり、演算部（MPU）、メモリ（RAM, ROM, EEPROM）、補助演算部（Co-processor）、乱数生成回路 100 を有する。ここで、補助演算部（Co-processor）は、暗号処理を実行する役割を有する。

#### 【0081】

乱数生成回路 100 において、本発明のシード生成回路と、例えば通常の擬似乱数生成回路などを組み合わせることにより、高品質の乱数を生成させることができる。この乱数生成回路 100 を搭載することで、演算部（MPU）や暗号処理専用の補助演算部（Co-processor）が常に高品質の乱数を読み出して使うこと

ができ、また、暗号鍵を IC の消費電流信号から読み出すハッキング技術に対する対策として、乱数を使って消費電流の変化を攪乱させることにも使え、高度な暗号セキュリティが実現可能となる。

図 13 は、本具体例の半導体集積回路 200 の回路規模を説明するための概念図である。すなわち、本発明のシード生成回路と、通常の擬似乱数生成回路などを組み合わせた乱数生成回路 100、全て CMOS 論理回路のみで構成できる。しかも論理ゲートの数は、わずか数 100 程度で済むので、各種の IC に搭載可能である。その回路規模は、図 13 に例示した程度あるいはそれ以下であり、IC 全体のサイズを大幅に増大させるという問題も生じない。

#### 【0082】

本発明の乱数生成回路を搭載することで、高度な暗号セキュリティ機能が利用可能になる。またゲーム機やモンテカルロシミュレーション用の乱数にも用いることができる。

#### 【0083】

(第 6 の具体例)

次に、本発明の第 6 の具体例として、本発明の乱数生成回路を搭載した IC カード及び携帯型の情報端末機器について説明する。

#### 【0084】

図 14 は、本具体例の IC カード及び情報端末機器を表す模式図である。すなわち、同図において 300 は、本具体例の IC カードまたは情報端末機器を表す。IC カードとしては、例えば、銀行の預金カードや各種のプリペイドカード、企業などにおける社員証、入門セキュリティカードなどを挙げることができる。また、情報端末器器としては、例えば、携帯電話や、その他の携帯型端末を挙げることができる。このような携帯型端末は、例えば、ワードプロセッサ、表計算、スケジューラ、ゲーム、電子メールの送受信、静止画や動画の撮影、などの各種の機能のうちのいずれかを備えたものを挙げることができる。

#### 【0085】

例えば、図 15 に表したような携帯電話 300 においても、本発明の乱数生成回路 100 を搭載することができる。またこれと類似した携帯型情報端末におい

ても同様である。

#### 【0086】

そして、本発明においては、シード生成回路と、通常の擬似乱数生成回路などとを組み合わせた乱数生成回路100を搭載することにより、非常に小型で消費電力も抑制しつつ高度な暗号セキュリティ機能を付加することができる。すなわち、乱数生成回路100を用いることにより、例えば、使用者の認証プロセスや、取り扱うデータの暗号化とその復元などをはじめとして、ゲーム機能に利用したり、モンテカルロシミュレーション用の乱数にも用いることができる。

以上、具体例を例示しつつ本発明の実施の形態について説明した。しかし、本発明は、上述した各具体例に限定されるものではない。

#### 【0087】

例えば、本発明において用いる発振回路、平滑回路、真性化回路、擬似乱数生成回路及び不確定論理回路の具体的な構成に関しては、上記の具体例に限定されず、その機能あるいは作用が同様な全ての回路に置換したのもも本発明の範囲に包含される。

#### 【0088】

例えば、出力が不確定なフリップフロップを複数個、並列もしくは直列に並べた論理回路を擬似乱数生成回路として用いることもできる。

#### 【0089】

また、本発明の乱数生成回路によって作られたデジタル乱数は、そのまま使用することもできるが、これをフィードバックシフトレジスタのシードとして用いることにより、新たな乱数を生成することもできる。

#### 【0090】

##### 【発明の効果】

以上詳述したように、本発明によれば、シード生成回路により、同一クロックデータ列に乱数性を持たせることが可能となり、これをシードに利用することで、同一クロックのデータ列においても高い乱数性を得ることができる。

#### 【0091】

連続発信する発信回路、平滑回路、ならびに真性化回路の各単位回路ブロック



を例えば図1の如く組み合わせることにより、同一クロックのデータ列が高い乱数性を持つことは、本発明以前には知られていなかった効果である。

#### 【0092】

しかも、本発明によれば、このような高品質の乱数を、フリップフロップ型の論理回路などを利用することにより少ない論理ゲート数で構成できるので、小規模な回路で済む。

#### 【0093】

すなわち、本発明によれば、真性度が高い乱数をコンパクト、低消費電力且つ低価格で実現できるようになり、例えばICカードや情報端末機器などに応用してセキュリティの確実な安価なシステムを実現できる点で産業上のメリットは多大である。

#### 【図面の簡単な説明】

##### 【図1】

本発明の実施の形態にかかるシード生成回路の要部構成を表すブロック図である。

##### 【図2】

発振回路10の具体例を表す模式図である。

##### 【図3】

発振回路10のもう一つの具体例を表す模式図である。

##### 【図4】

本発明における平滑回路20の基本的な構成を表すブロック図である。

##### 【図5】

真性化回路30の作用を説明するための模式図である。

##### 【図6】

本発明の第1の具体例にかかるシード生成回路を表すブロック図である。

##### 【図7】

第1具体例のシード生成回路を統計的な検定にかけた結果を表す一覧表である。

##### 【図8】

8個のシード生成回路について、システム起動後のクロック数と乱数データの各1ビットについて、一様性の改善の傾向を表すグラフ図である。

【図9】

本発明の第2の具体例にかかるシード生成回路を表す模式図である。

【図10】

本発明の具体例にかかるシード生成回路を表す模式図である。

【図11】

本発明の具体例にかかる乱数生成回路を表す模式図である。

【図12】

本発明の具体例の半導体集積回路の要部構成を表す模式図である。

【図13】

本発明の具体例の半導体集積回路200の回路規模を説明するための概念図である。

【図14】

本発明の具体例の情報端末機器を表す模式図である。

【図15】

本発明の情報端末機器としての携帯型電話である。

【図16】

同一クロックデータ列における乱数性を説明するための概念図である。

【図17】

擬似乱数回路におけるシードの役割を説明するための概念図である。

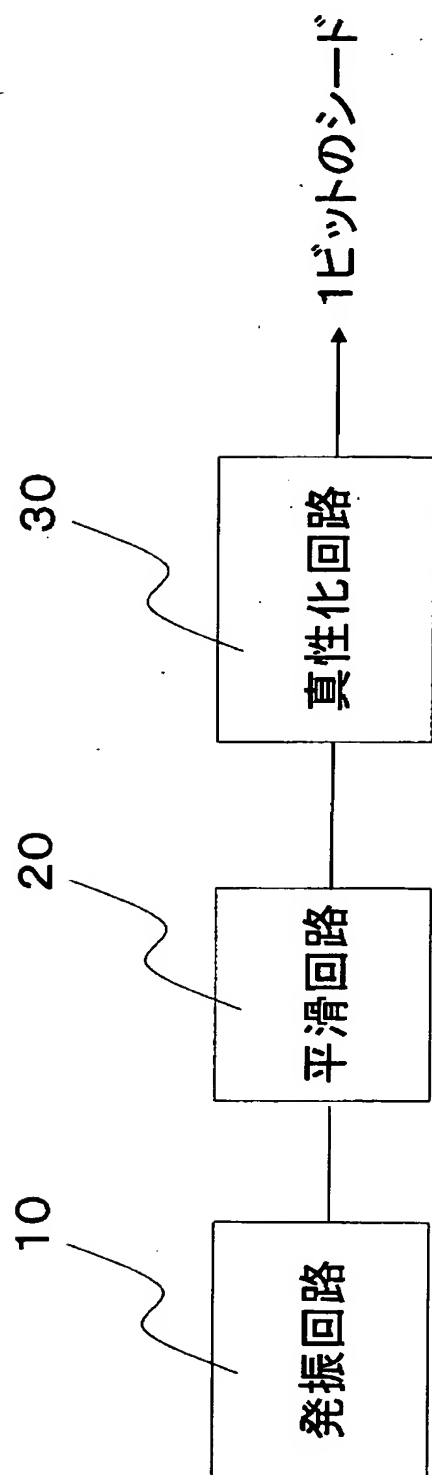
【符号の説明】

- 100 乱数生成回路
- 110 シード生成回路
- 120 擬似乱数生成回路
- 130 不確定論理回路
- 200 半導体集積回路
- 300 ICカード及び情報端末機器

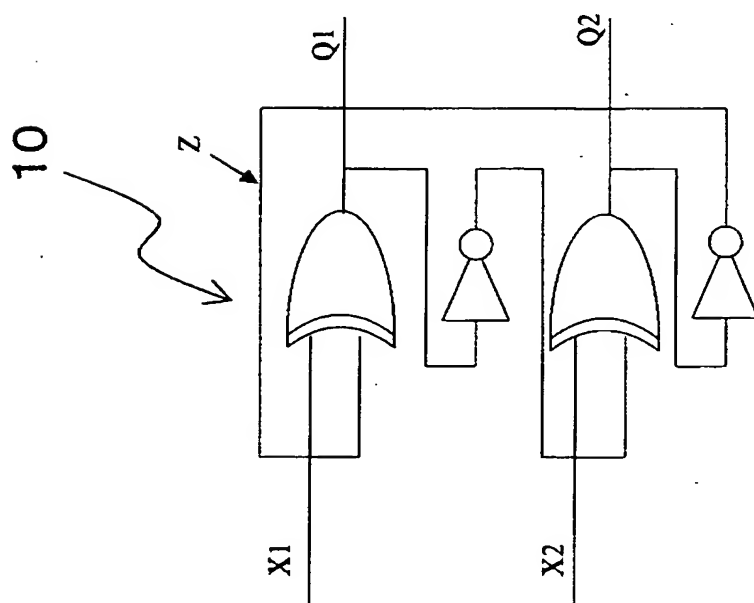
【書類名】

図面

【図 1】

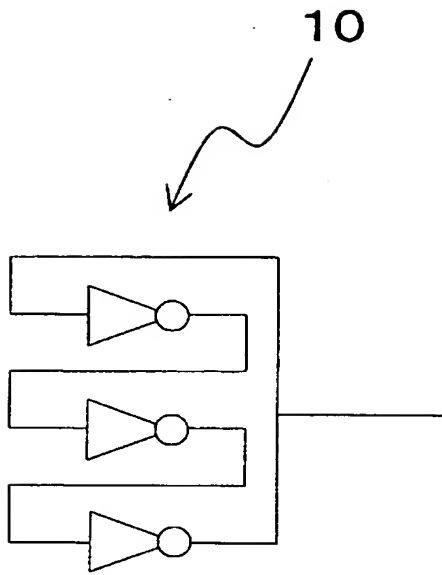


【図 2】

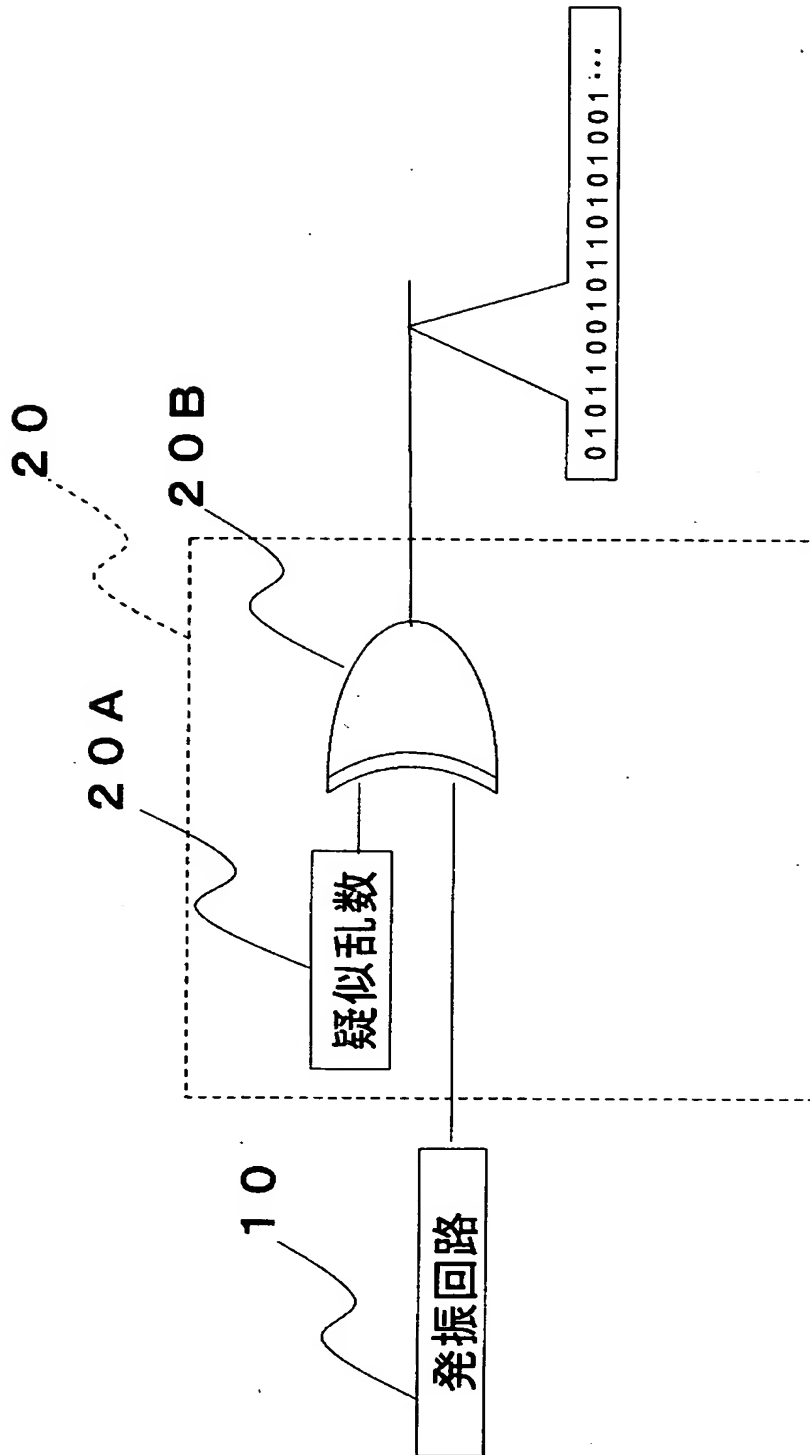


If  $X1 = X2$ ,  
 フリップフロップ (インバータが偶数個) と等価  
 $Z=1$  のとき  
 ・  $X1 = X2 = 1$  ならば  $Q1=0$ ,  $Q2=0$   
 ・  $X1 = X2 = 0$  ならば  $Q1=1$ ,  $Q2=0$   
 $Z=0$  のとき  
 ・  $X1 = X2 = 1$  ならば  $Q1=1$ ,  $Q2=1$   
 ・  $X1 = X2 = 0$  ならば  $Q1=0$ ,  $Q2=1$   
 If  $X1 \neq X2$ ,  
 リング発振器と等価

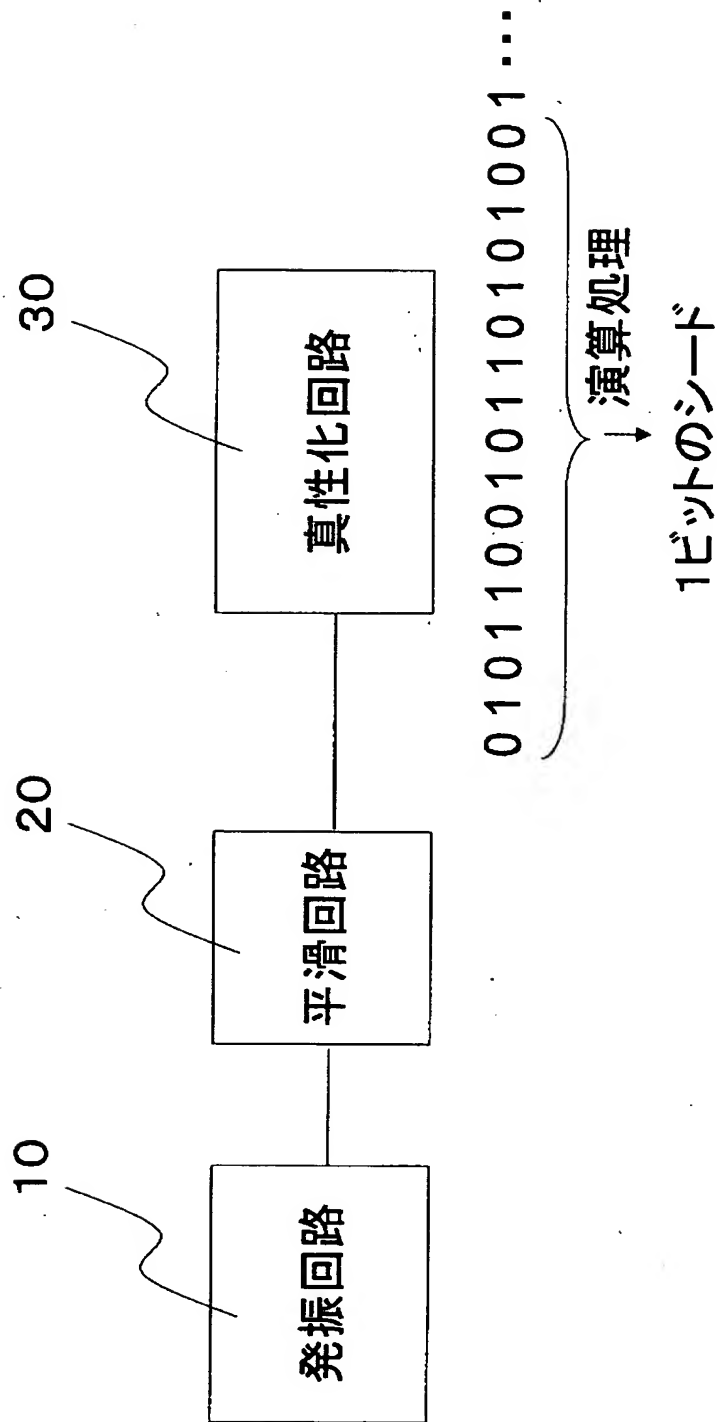
【図 3】



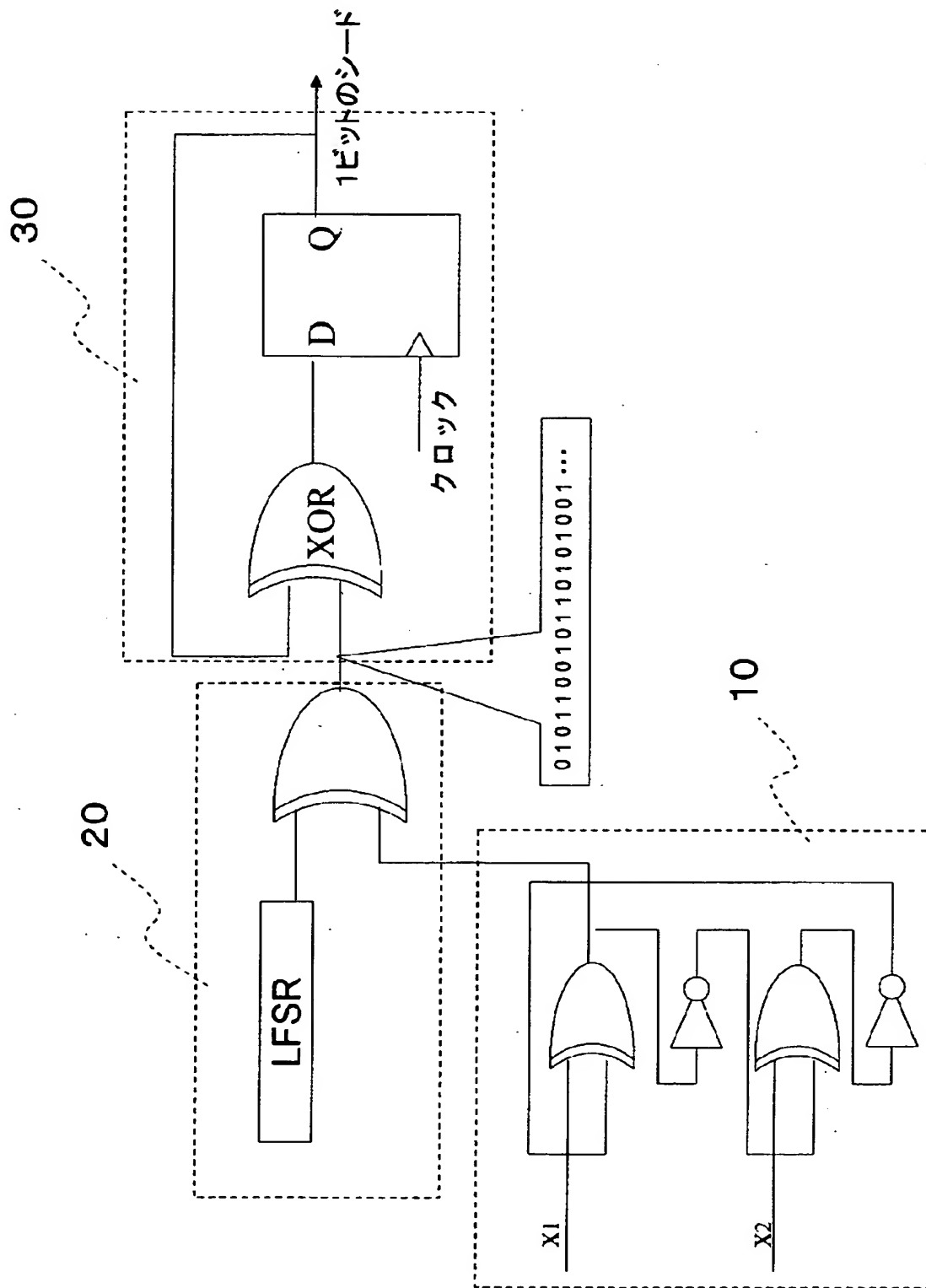
【図 4】



【図 5】



【図 6】



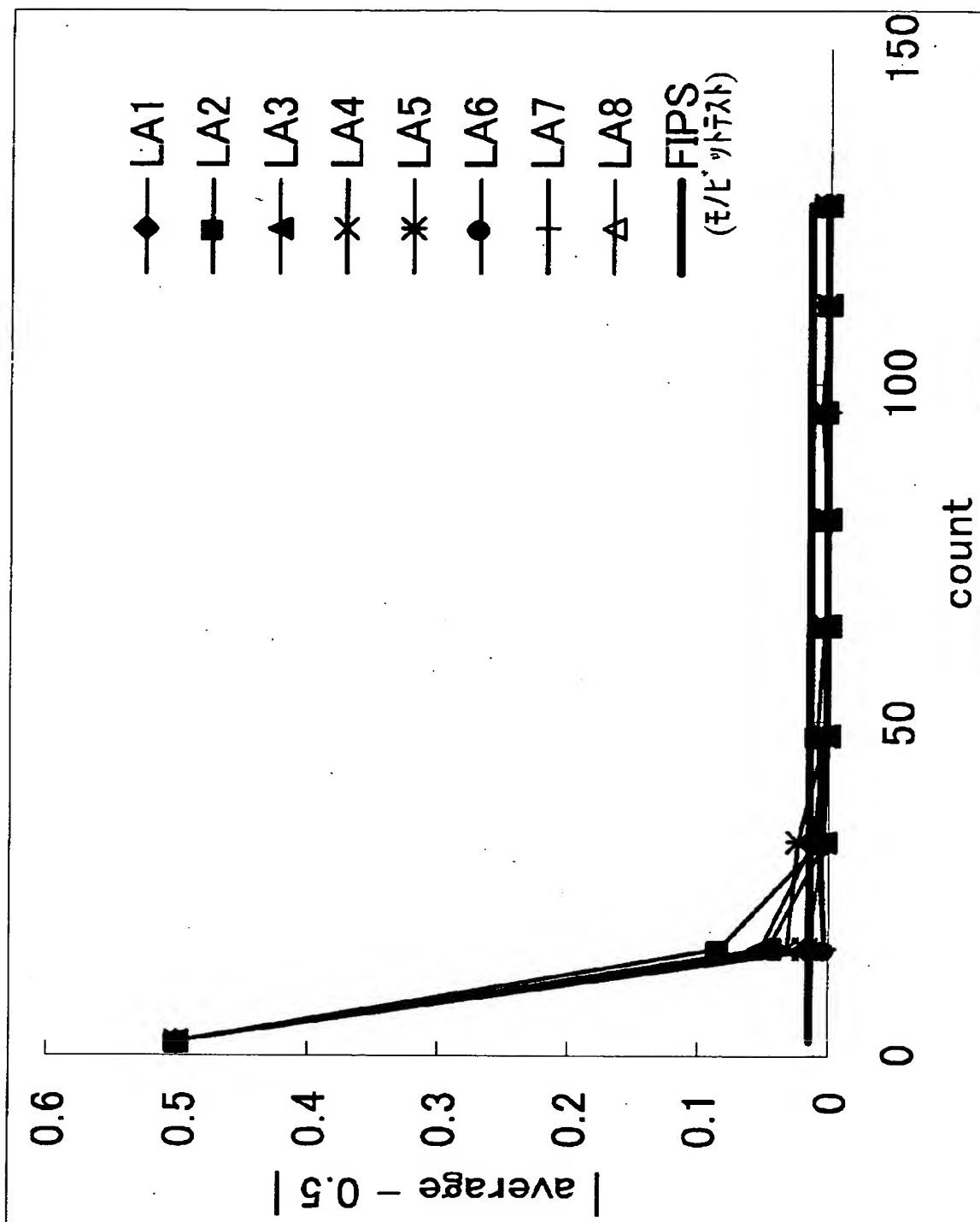


【図 7】

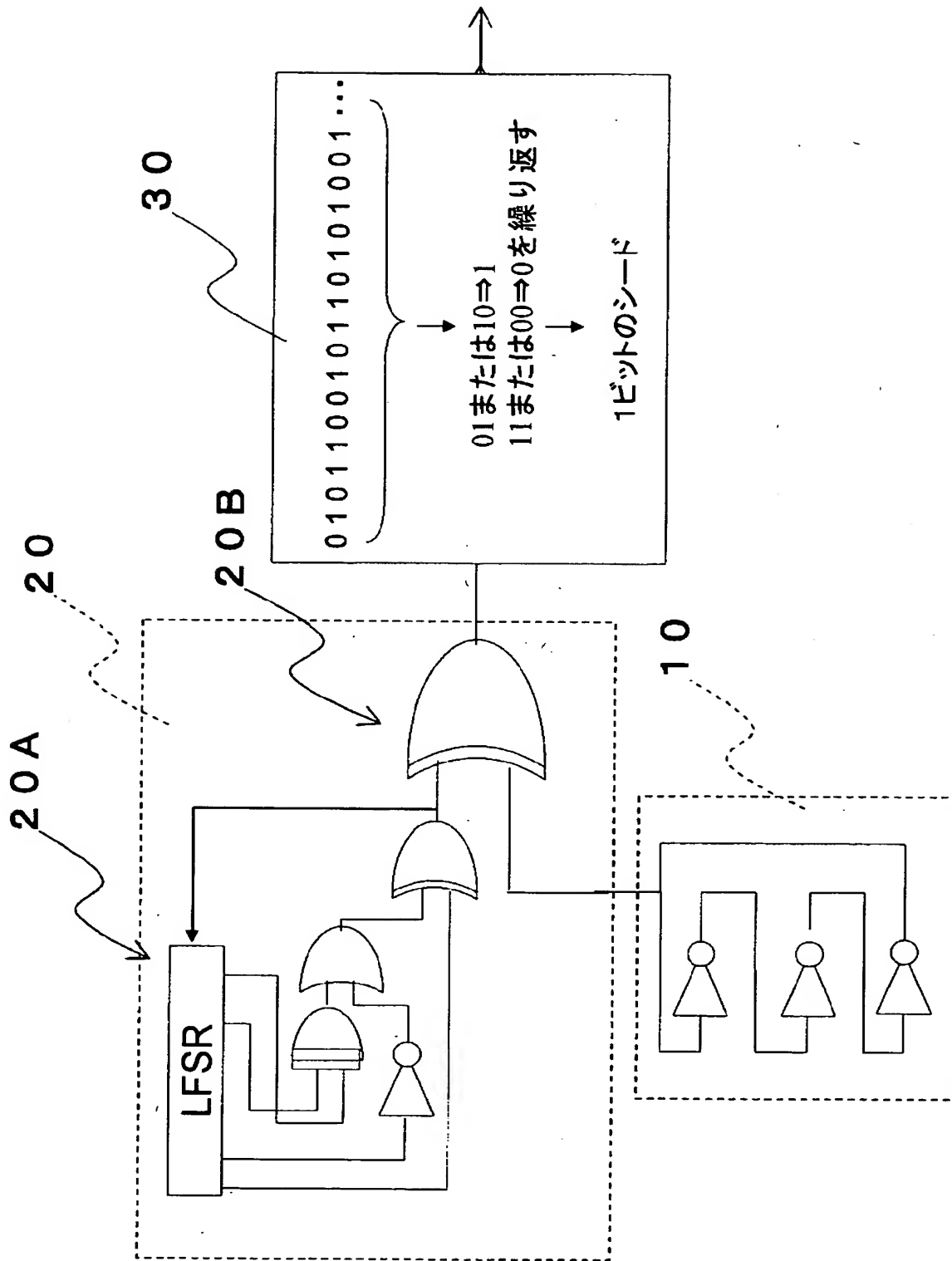
<FIPS140-2>	20000data	熱雑音増幅型	擬似乱数 (16段 LFSR)	本提案
Monobit	9725 ~ 10275: 10000±275	10059 ◎	×	10221 ○
Run1	2315 ~ 2685: 2500±185	2588 2564 ◎	×	2584, 2498 ◎
Run2	1114 ~ 1368: 1241±127	1282 1246 ◎	×	1284, 1264 ◎
Run3	527 ~ 723: 625±98	610, 650 ◎	×	593, 595 ◎
Run4	240 ~ 384: 312±72	302, 327 ◎	×	316, 349 ◎
Run5	103 ~ 209: 156±53	148, 139 ◎	×	145, 176 ◎
Runover6	103 ~ 209: 156±53	144, 148 ◎	×	120, 160 ◎
Poker test	2.16(X<46.17: 24.165±22.005	10.22 ◎	×	20.6336 ◎
long run	longest run < 26		×	14, 17 ◎
<General test>	8000data		×	
$\chi^2$ 乗検定	QK > 0.05	0.14 △	×	0.202465 ○
Run test	Pv > 0.01	0.153 ○	×	0.543148 ◎
Freq. Test in block	QK > 0.05	0.745 ◎	×	0.217996 ◎
Poker Test	QK > 0.05	0.272 ◎	×	0.510356 ◎
Serial Cor. Test	-0.022491 < C < 0.02241	-0.0163 △	×	-0.007205 ◎
Gap test:0	QK > 0.05	0.901896 ◎	×	0.664227 ◎
Gap test:1	QK > 0.05	0.19484 ◎	×	0.591764 ◎
Gap test:2	QK > 0.05	0.56847 ◎	×	0.849706 ◎
Gap test:3	QK > 0.05	0.89883 ◎	×	0.017445 ◎
Gap test:4	QK > 0.05	0.849298 ◎	×	0.220639 ◎
Gap test:5	QK > 0.05	0.615556 ◎	×	0.315313 ◎
Gap test:6	QK > 0.05	0.333719 ◎	×	0.004307 ◎
Gap test:7	QK > 0.05	0.629796 ◎	×	0.466615 ◎
Gap test:8	QK > 0.05	0.281213 ◎	×	0.218405 ◎
Gap test:9	QK > 0.05	0.879929 ◎	×	0.072952 ○
Gap test:10	QK > 0.05	0.339877 ◎	×	0.656671 ◎
Gap test:11	QK > 0.05	0.57006 ◎	×	0.633447 ◎
Gap test:12	QK > 0.05	0.112747 ◎	×	0.743529 ◎
Gap test:13	QK > 0.05	0.885725 ◎	×	0.787189 ◎
Gap test:14	QK > 0.05	0.080402 ○	×	0.485003 ◎
Gap test:15	QK > 0.05	0.747962 ◎	×	0.931562 ◎

◎余裕もって合格(QK&gt;0.1) ○合格 △▲ボーダーで合否 ×失格

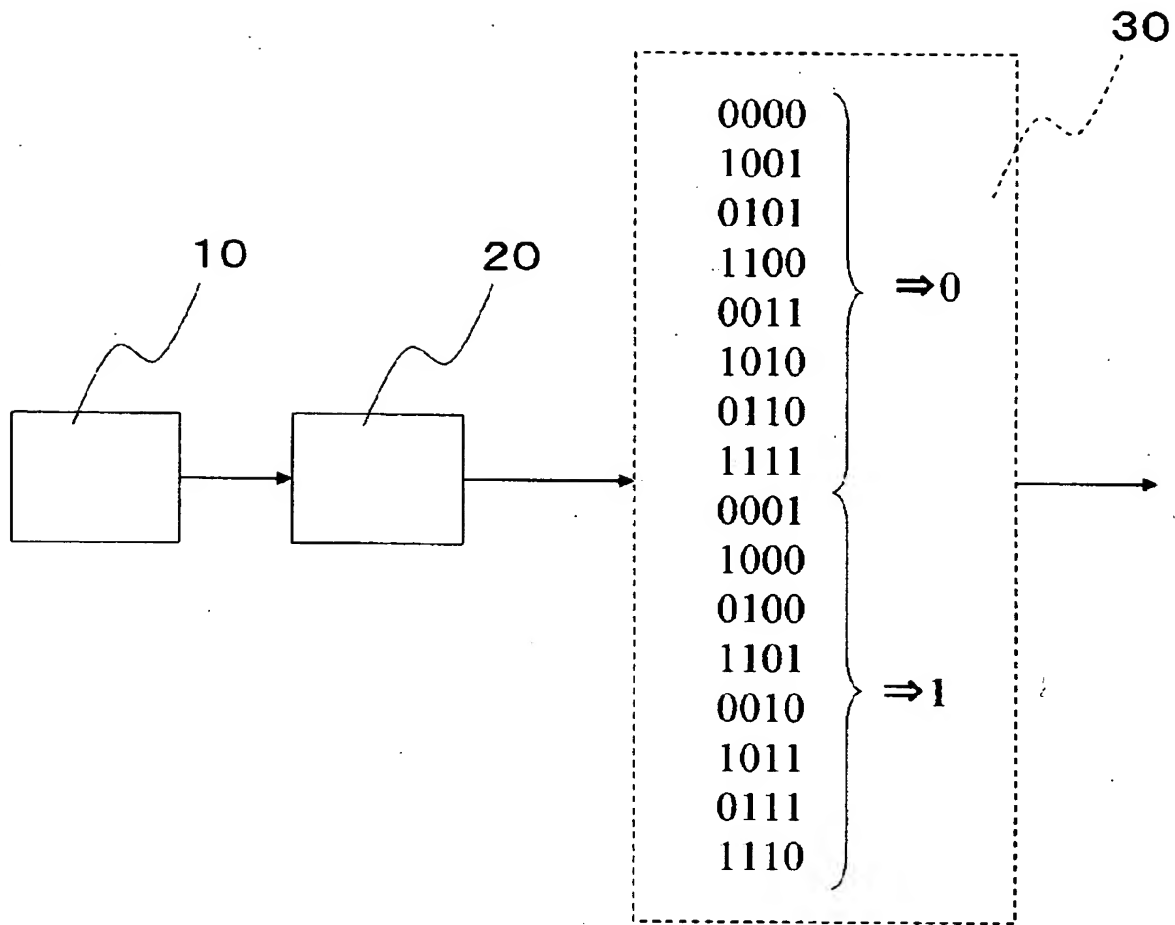
【図 8】



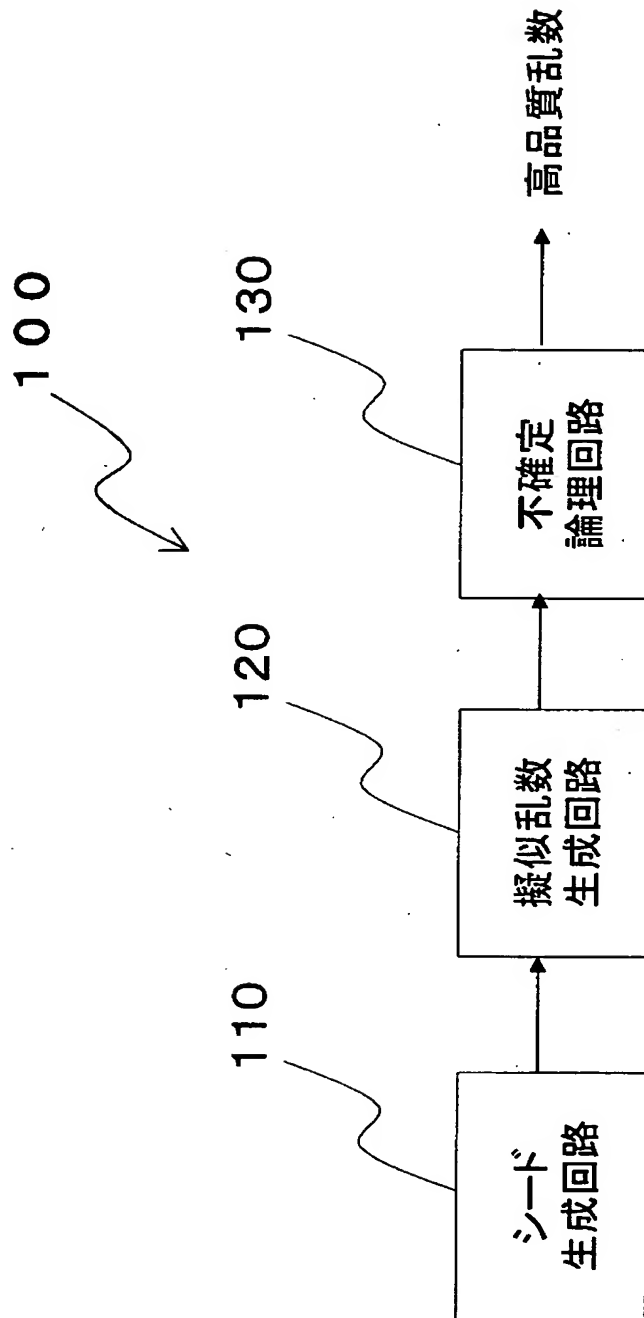
【図 9】



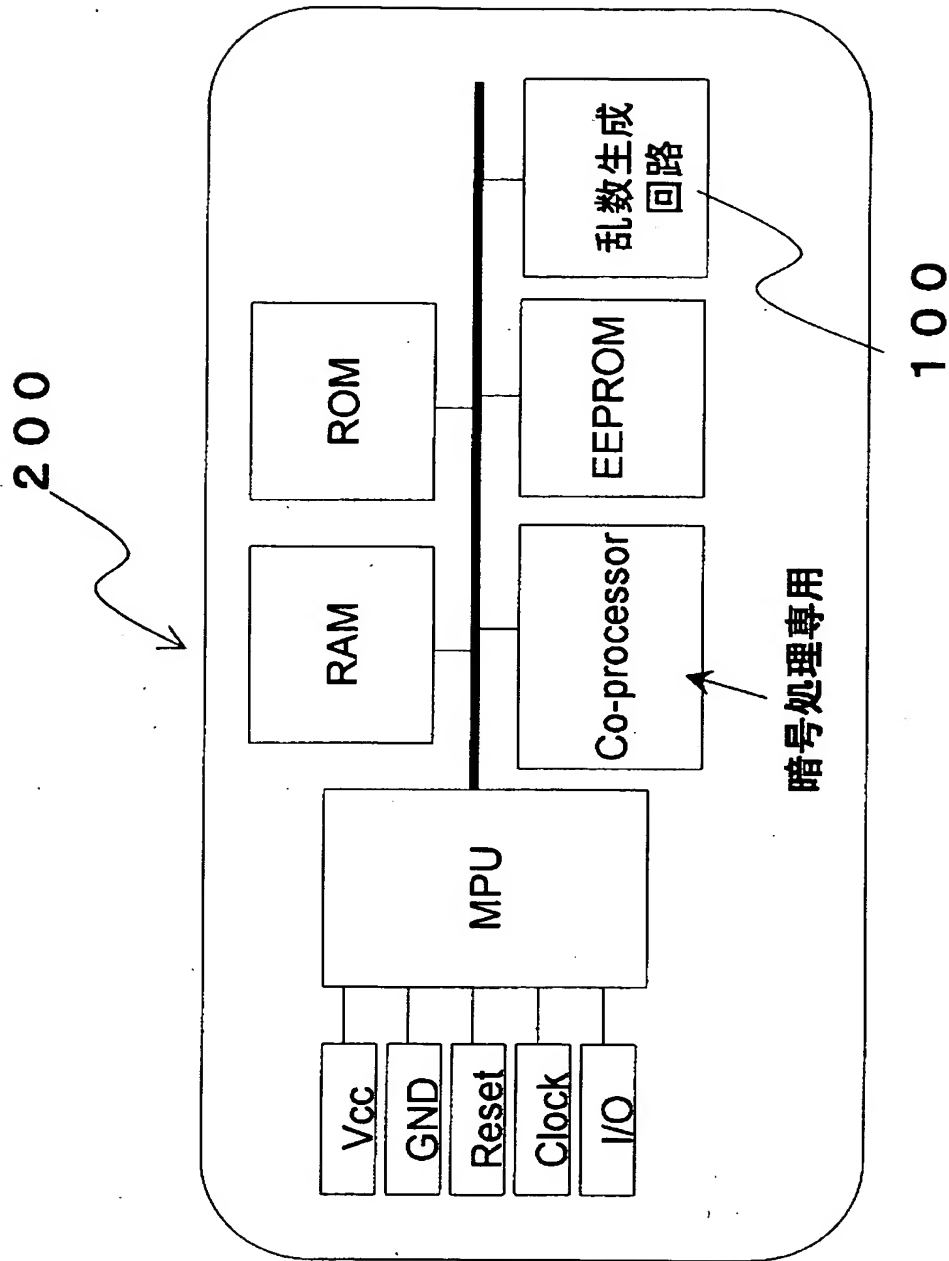
【図 10】



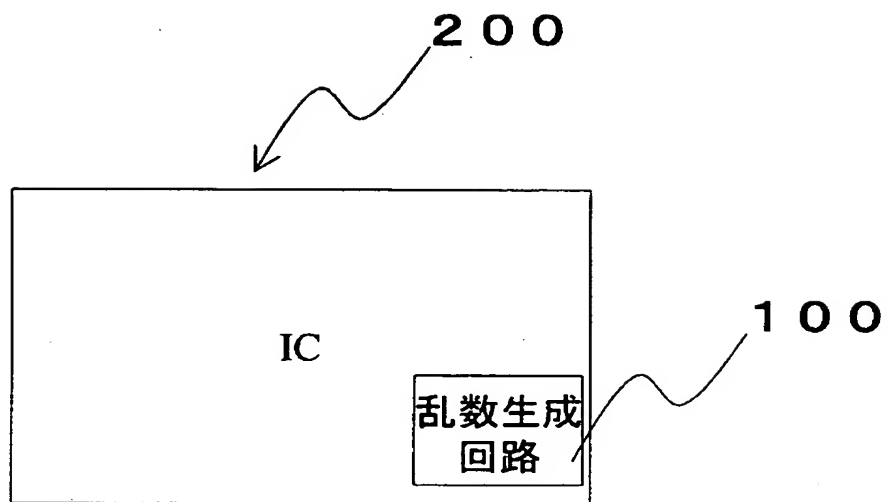
【図 11】



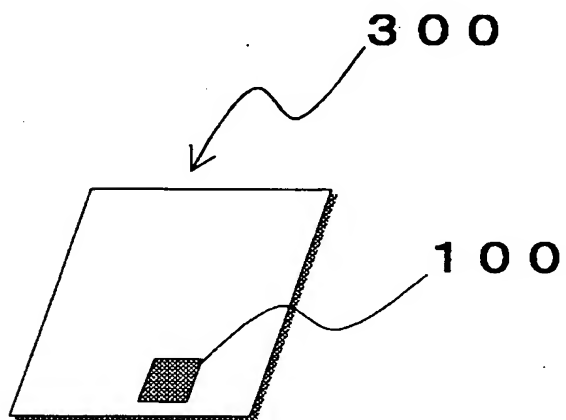
【図 12】



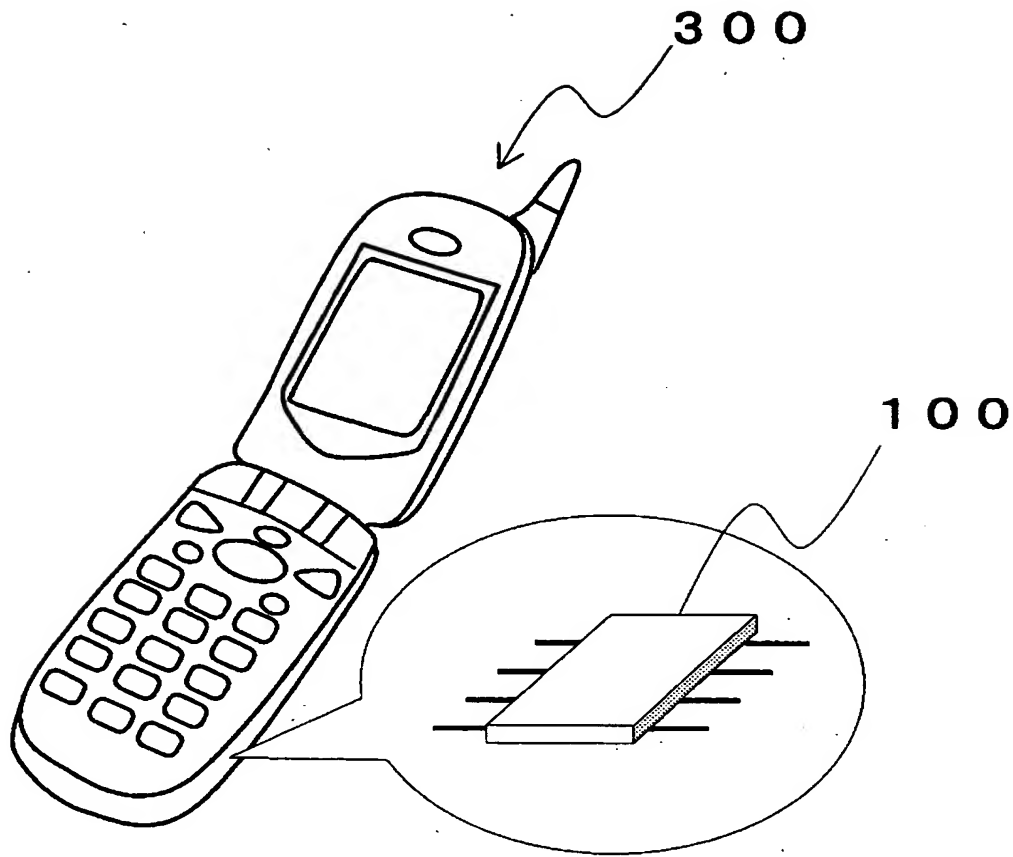
【図 13】



【図 14】

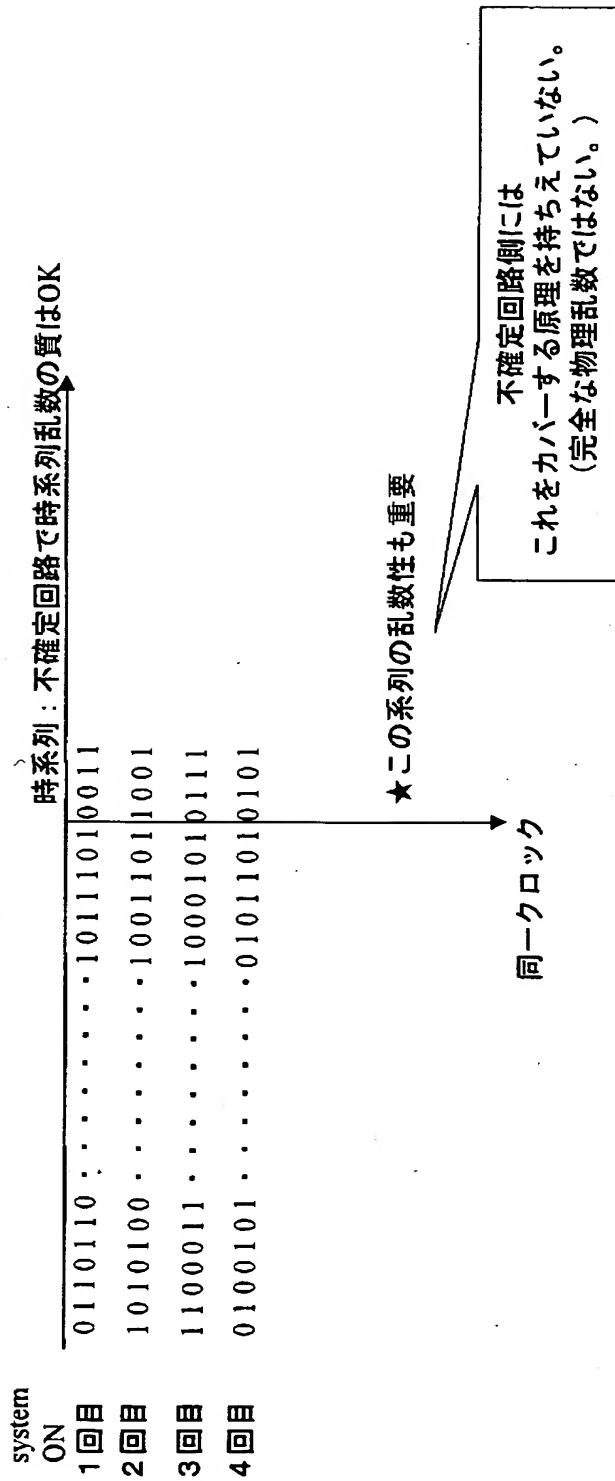


【図 15】

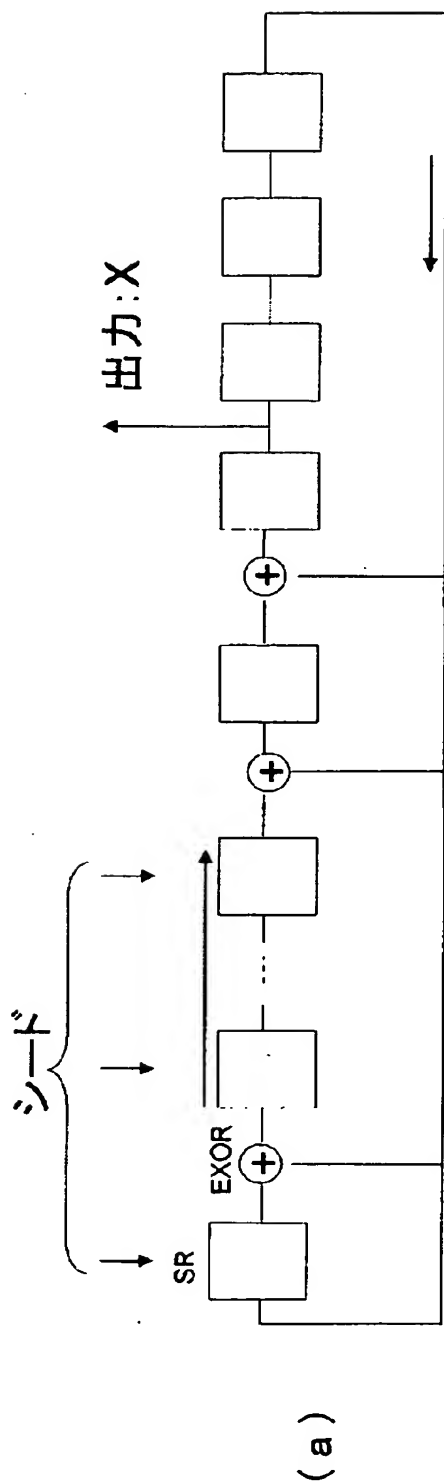




【図 16】



【図 17】



																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																		</
--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	----

時系列

X:1回目	0	1	0	1	1	0	0	1	0	1	1	0	1	0	0	1	...
2回目	1	0	0	0	1	0	1	1	0	1	0	0	0	0	0	1	...
3回目	0	1	0	1	0	0	0	1	1	1	1	0	0	0	1	0	...
4回目	1	1	1	0	1	1	0	0	1	0	1	0	1	1	1	0	...

システム起動後の同一クロックサンプリングの乱数性=シードに依存

【書類名】 要約書

【要約】

【課題】 乱数性の高いシードを生成し、かつ小型の集積回路化が可能なシード生成回路及びこれを用いた乱数生成回路、半導体集積回路、ICカード及び情報端末機器を提供することを目的とする。

【解決手段】 連続的または断続的に発振する発振回路（10）と、前記発振回路から出力されたデジタルデータ列における「0」と「1」との出現頻度を制御して時系列データとして出力する平滑回路（20）と、前記時系列データのうちの複数のビットを用いた演算処理により、1ビットのシードを生成する真性化回路（30）と、を備えたことを特徴とするシード生成回路を提供する。

【選択図】 図1

特願 2003-019732

出願人履歴情報

識別番号

[000003078]

1. 変更年月日

2001年 7月 2日

[変更理由]

住所変更

住 所

東京都港区芝浦一丁目1番1号

氏 名

株式会社東芝

2. 変更年月日

2003年 5月 9日

[変更理由]

名称変更

住所変更

住 所

東京都港区芝浦一丁目1番1号

氏 名

株式会社東芝